

Certification of CPNI Filing - February 6, 2006

WC Docket No 05-196 EB-06-TC-060 DA- 06-23

This certification is filed in compliance of the Commission's requirement as set forth by section 64.2009(e) of the Commission's rules.

As required by Section 222 of the Communications Act of 1934, as amended; PageMe! Inc, is a wireless paging carrier; and its affiliated companies (Mountain Communications, Inc.; Communications Unlimited; PageOne Wireless), along with its contractual sales agents, do hereby certify that we protect the privacy of customer proprietary network information ("CPNI"), and the privacy of customer proprietary billing information.

We have procedures in place to protect all customer information. We train our employees on the procedures in effect to protect all customer information. Attached with this certification, is a copy of our procedures that insures the privacy of customer proprietary network information.

Questions or inquiries should be directed to the office of our President.

David Balsick, President

PageMe! Inc.



Customer Privacy Policy

PageMe! Inc., its employees, affiliated companies, agents and subcontractors will strictly follow the following guidelines to Protect & Safeguard our Customer's Proprietary Network Information and Billing Information.

- 1. A hard file will be kept per customer, and will include all original contracts, customer change orders, billing resolutions, information inquiries, correspondence, and related materials. No information contained within the customer records (electronic or hard file) will be divulged to any party without the written permission of the President of PageMe! Inc. No hard file is to be removed from the protected and secure filing area. No hard file and/or electronic file shall be copied and/or distributed without the written permission of the President of PageMe! Inc.
- 2. Customer billing records are private information. All verbal communications with the customer will be kept as electronic file posting notes, within the billing file records, accessible only by authorized personnel, under password protection. No information will be provided to third party entities for any sales marketing.
- 3. Customer proprietary network information (paging information records, paging terminal logs, paging delivery logs, iServ logs, SurePage logs) records are private information. Access to this information shall be accessible only by authorized personnel, under password protection. All information is to be held in strict confidence.
- 4. Requests for billing and/or customer network information, must be recorded on a customer service order, must include the customer name, address, telephone number, billing account number, unit number, requesting persons name, the range of specific information requested, and the reason for the request. If the customer request for information is in person, then they must sign the customer service order, else they must provide the personal passcode associated with the account.
- 5. Customer service personnel must obtain validation information from the requesting person. The requesting party must provide the personal passcode on file, or two other forms of identification Driver's license or other valid forms of identification; PMI numbers, verifiable customer record information, etc. If the customer service personnel can not be provided with the mandatory information, inform the caller that the requested information can not be provided.
- 6. Completed requests, and / or any formal written request for information by any local government, municipal, city, state or federal agency, will be directed to the office of the President of PageMe! Inc., ONLY.
- 7. Upon review of the information request, the President of PageMe! Inc. will contact the requesting party to further verify the requested information and confirm the request. If all information is verified, the President of PageMe! Inc. will consider fulfilling the information request, and will personally attest to its accuracy and security of delivery to the requesting party.
- 8. A copy of all provided information will be included in the customer hard file. All customer files will be maintained a minimum of 3 years, after the file becomes inactive.
- 9. Any breach of information, will be promptly reported to the President of PageMe! Inc. A detailed incident written report will be generated within the same business day, and submitted to the President of PageMe! Inc.
- 10. Failure to follow these security procedures, and/or a breach of security information, will result in a disciplinary review of the employee or employees. Disciplinary action may include immediate termination.
- 11. Direct all questions to the President of PageMe! Inc.

Revised 11/2005